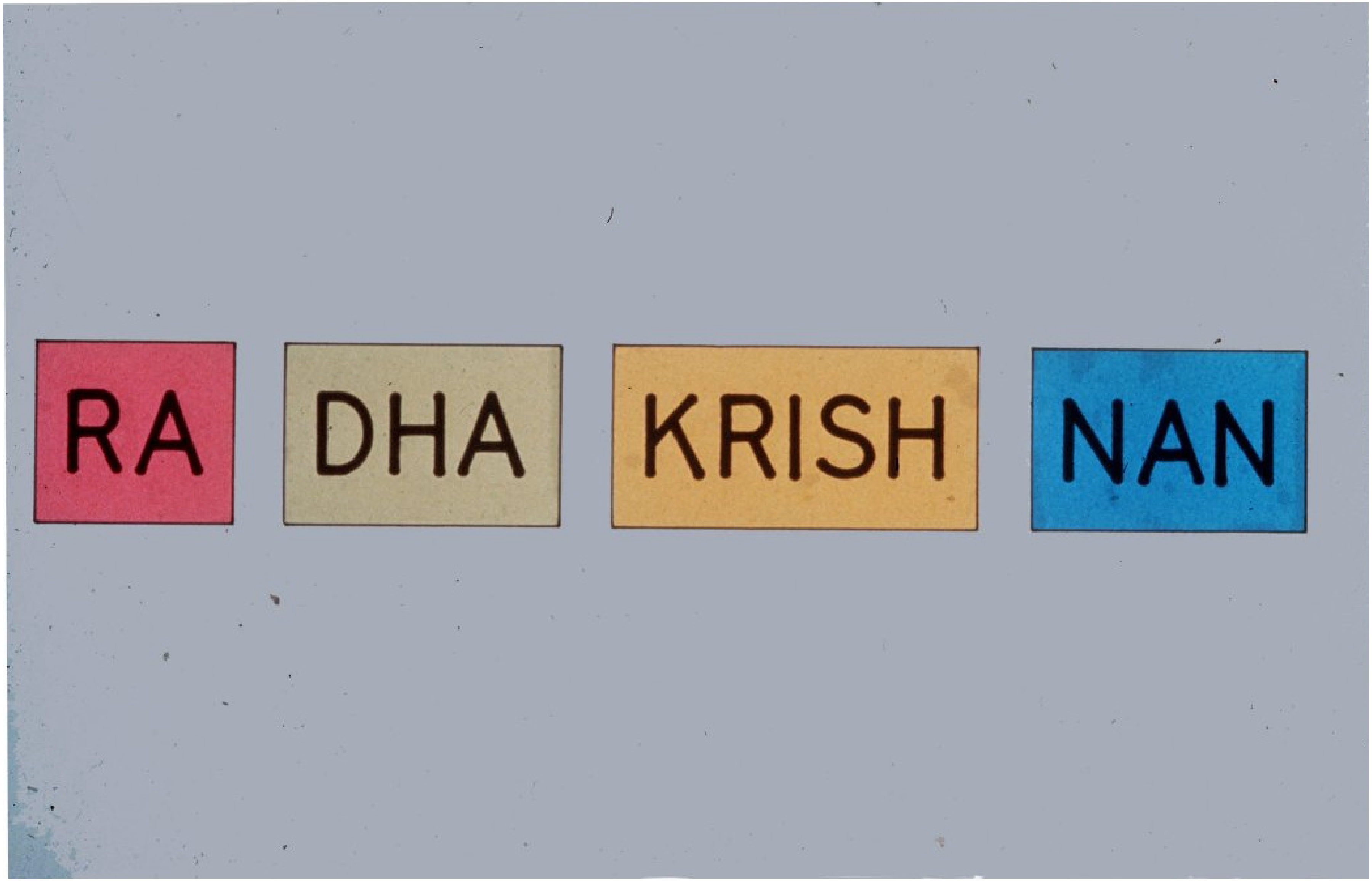
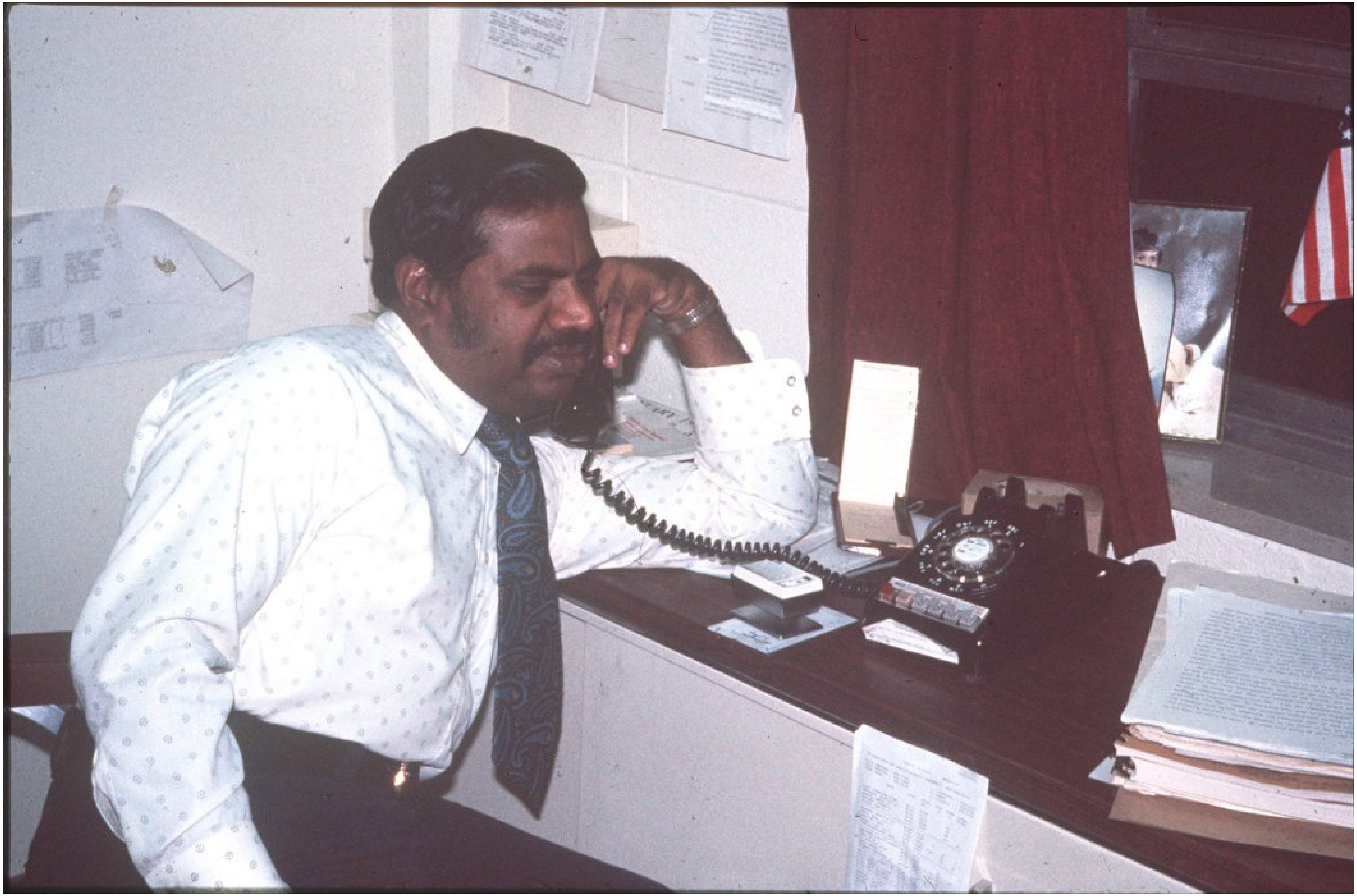
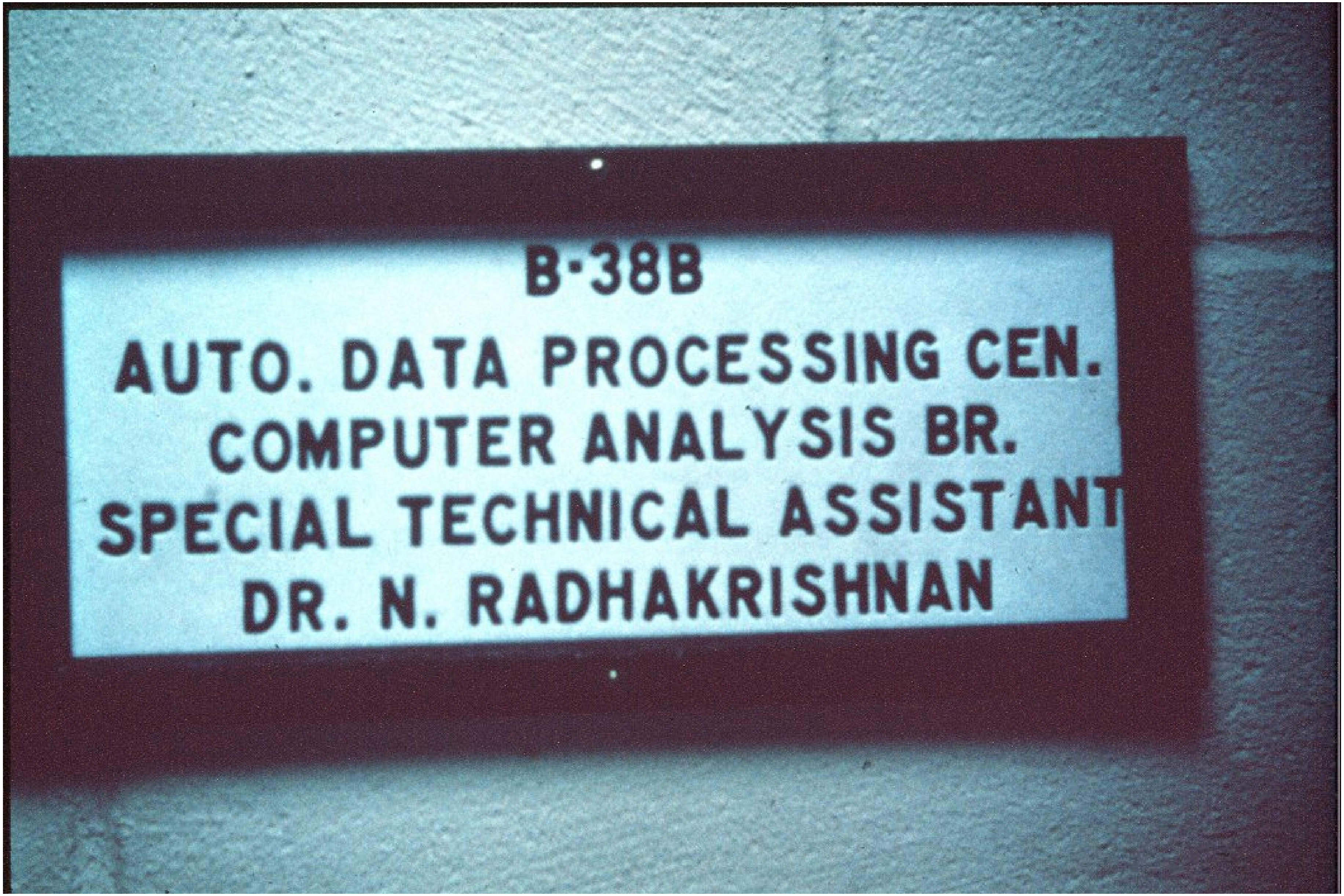
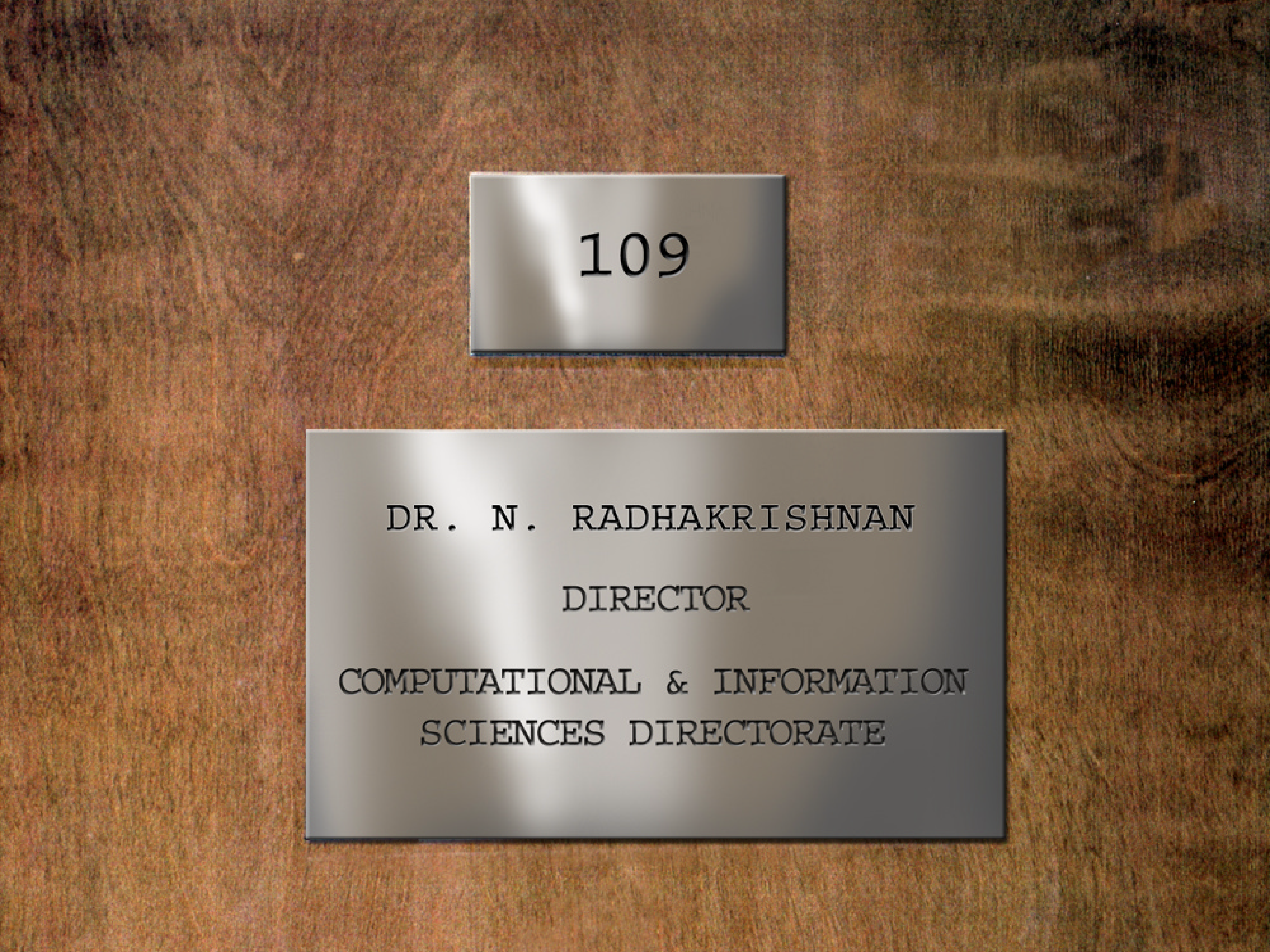


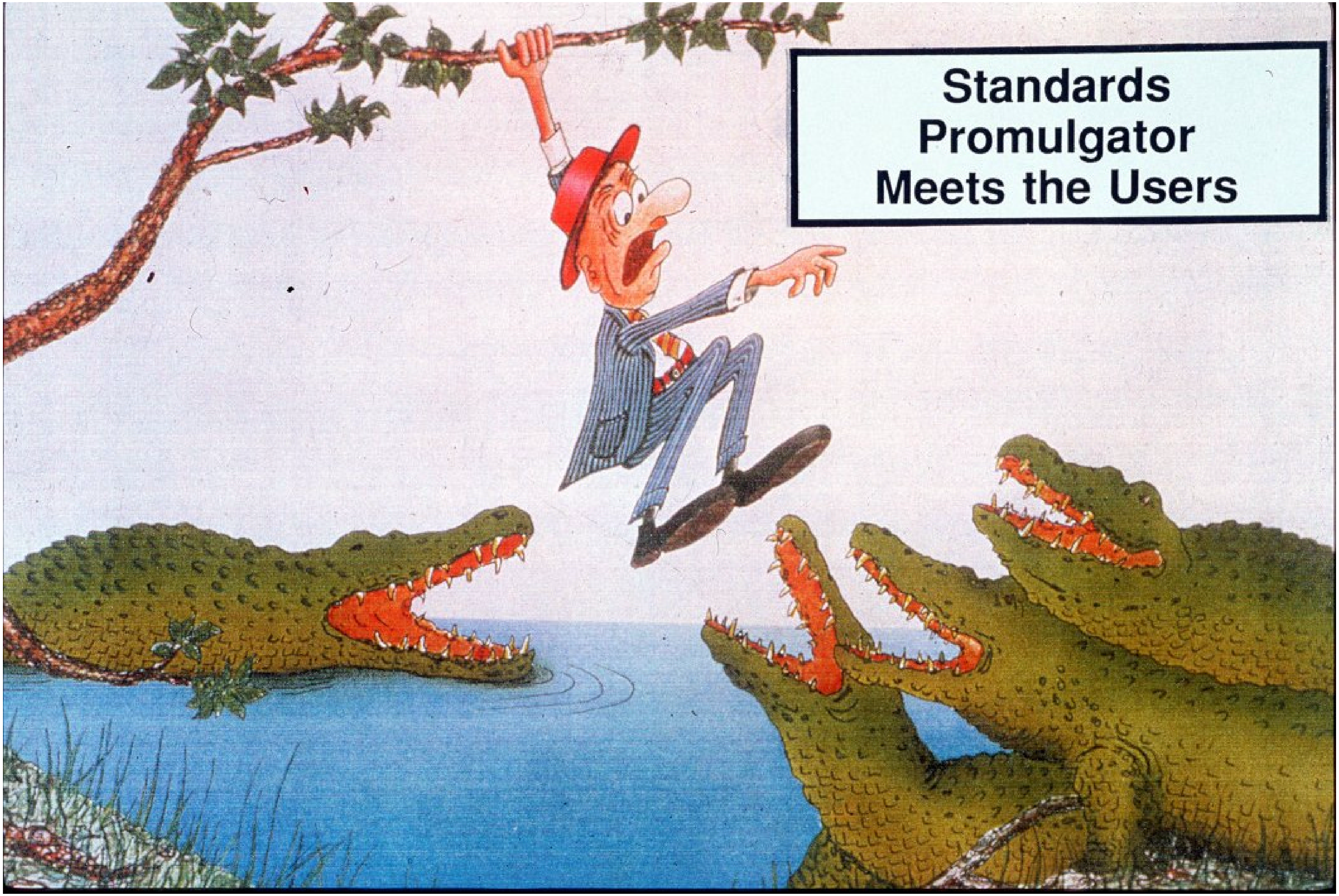
RA DHA KRISH NAN





B-38B
AUTO. DATA PROCESSING CEN.
COMPUTER ANALYSIS BR.
SPECIAL TECHNICAL ASSISTANT
DR. N. RADHAKRISHNAN


109
DR. N. RADHAKRISHNAN
DIRECTOR
COMPUTATIONAL & INFORMATION
SCIENCES DIRECTORATE

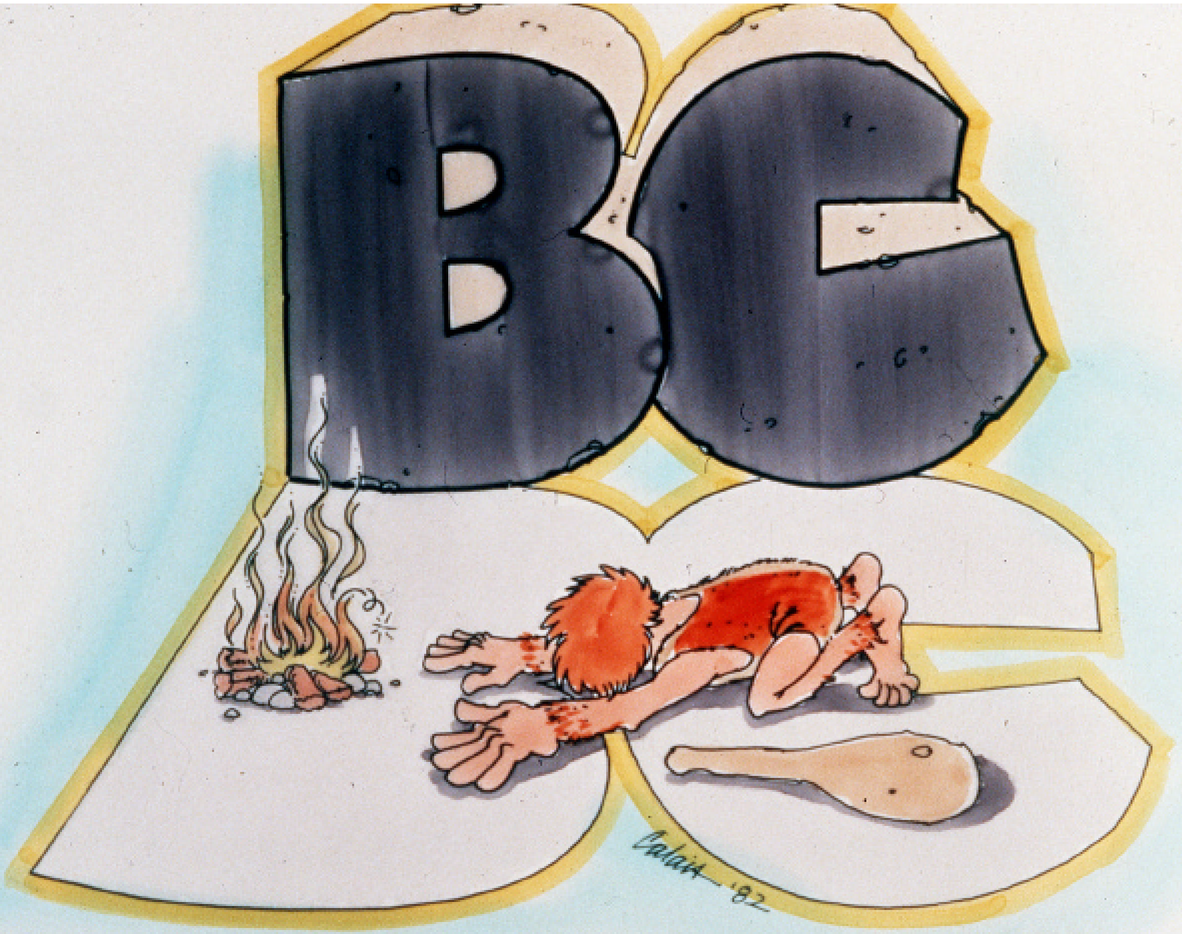


Standards Promulgator Meets the Users

Information Assurance

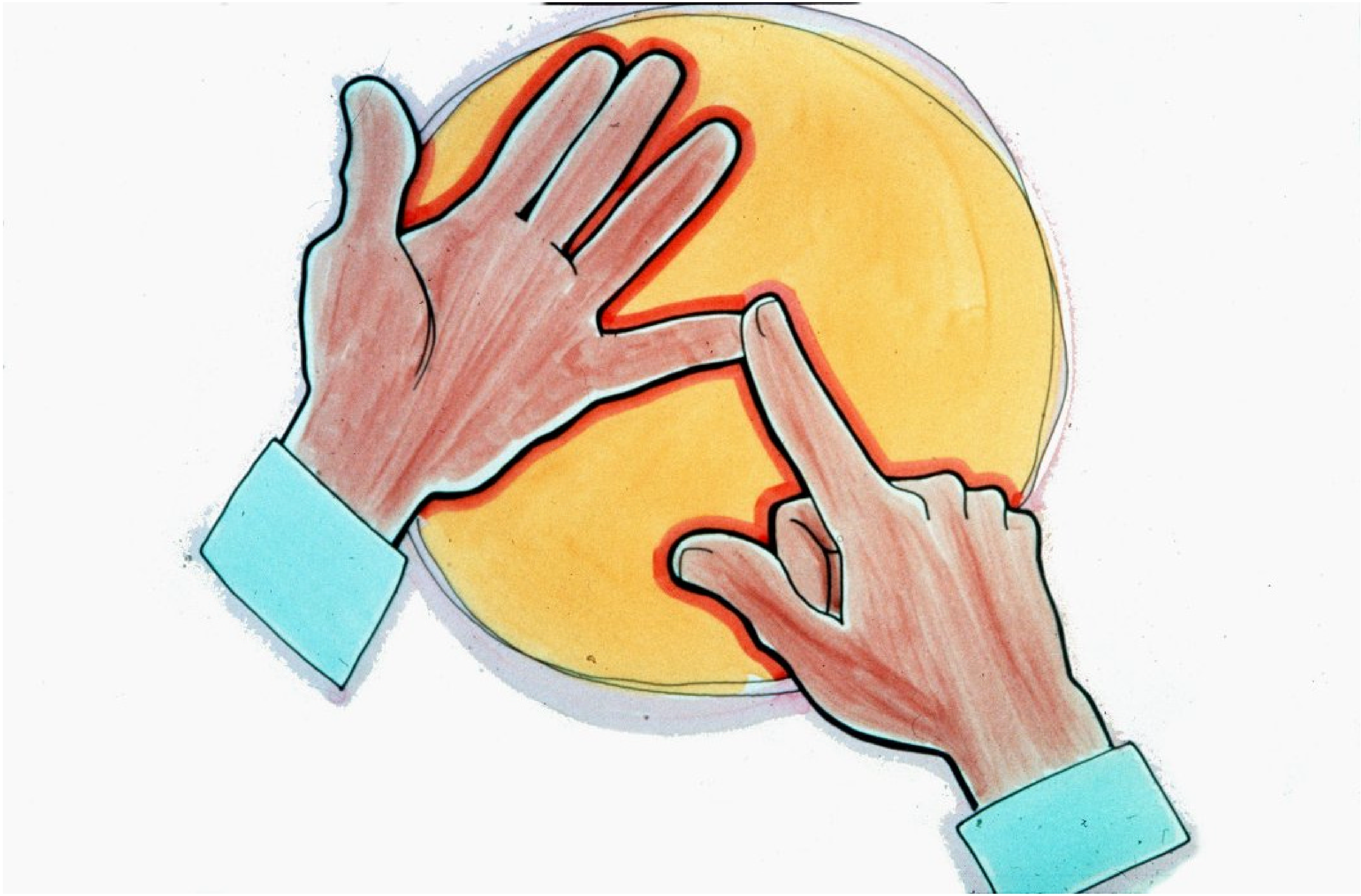
National Defense Industrial Association

February 25 - March 1, 2002

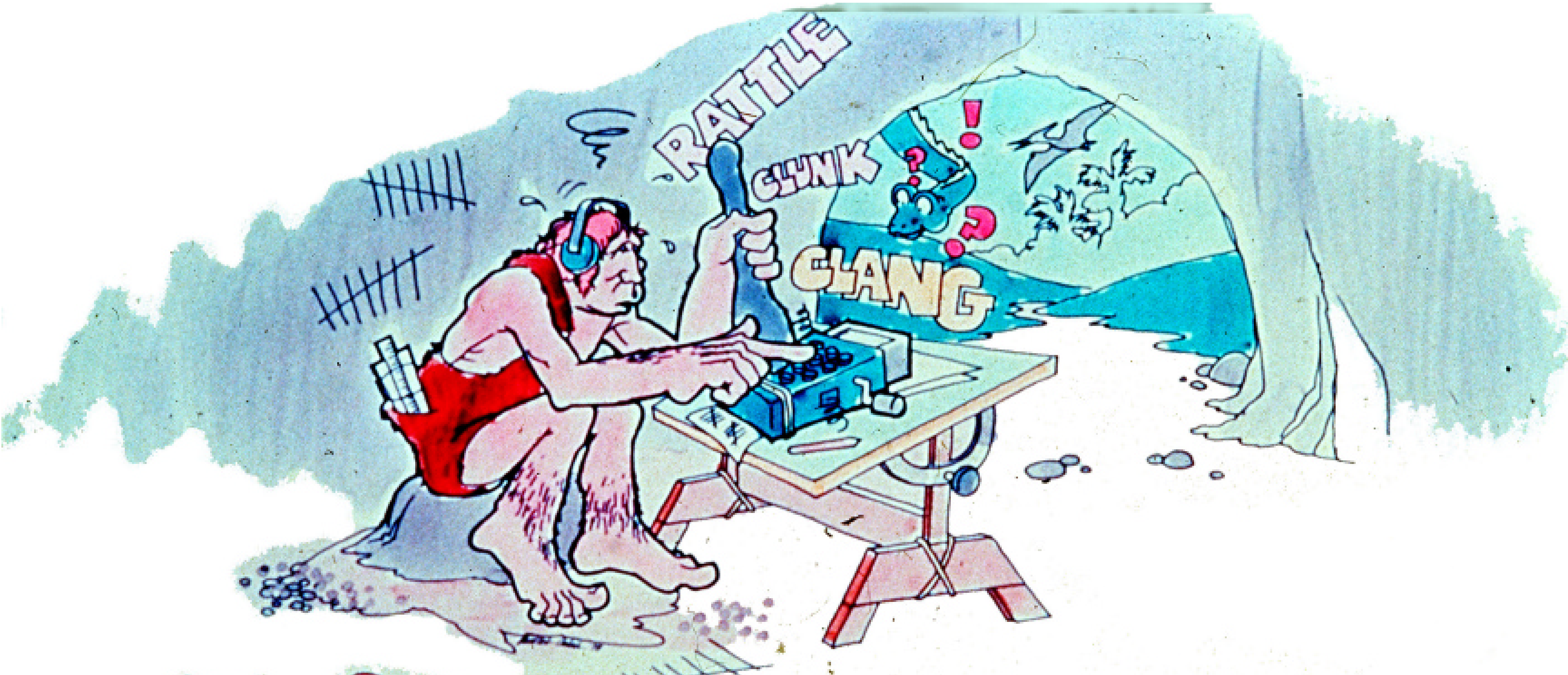


Before Christ

Before Computers

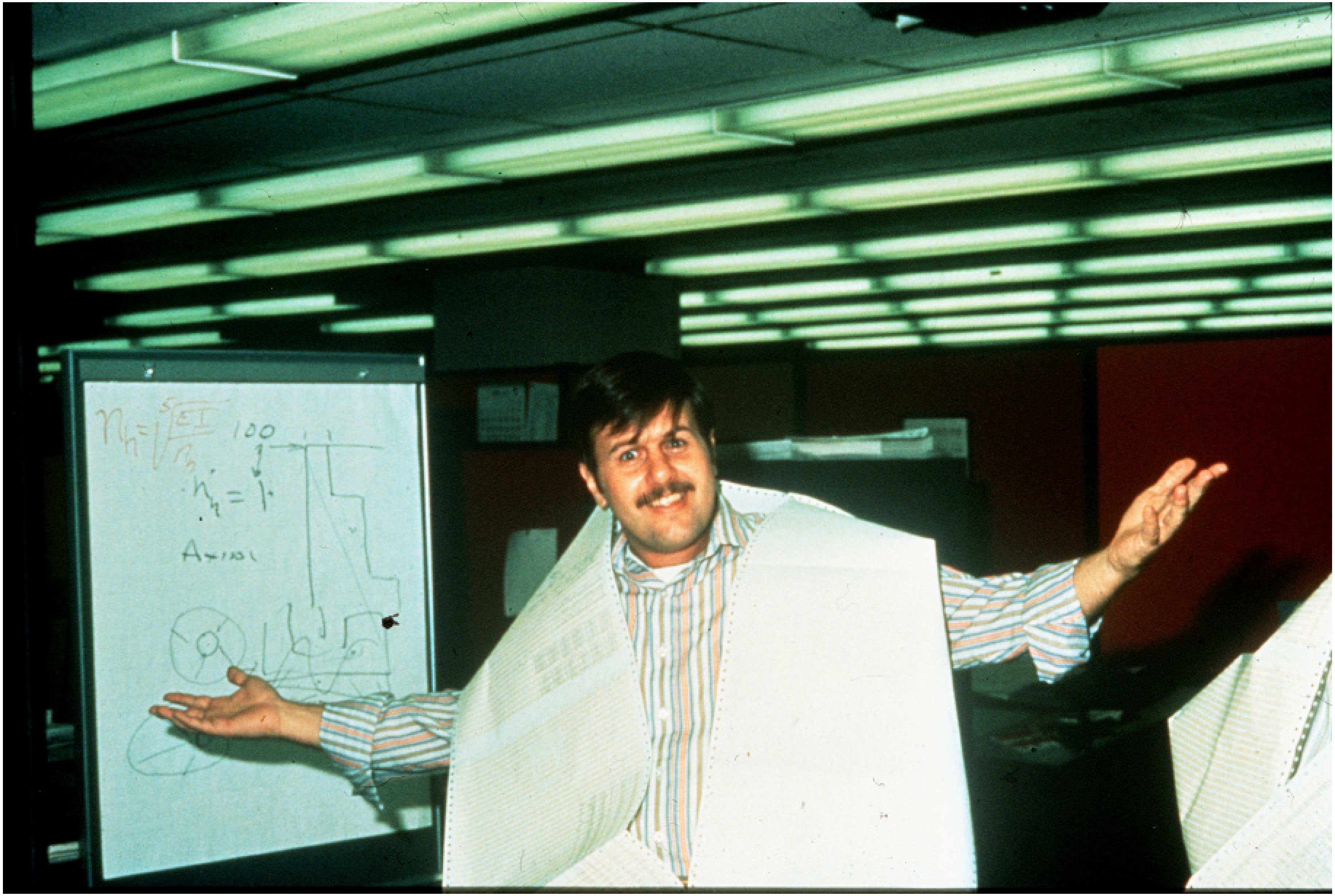


1 2 3 4 5 6 7 8 9 10 11 12... er? 13...
PHEW!

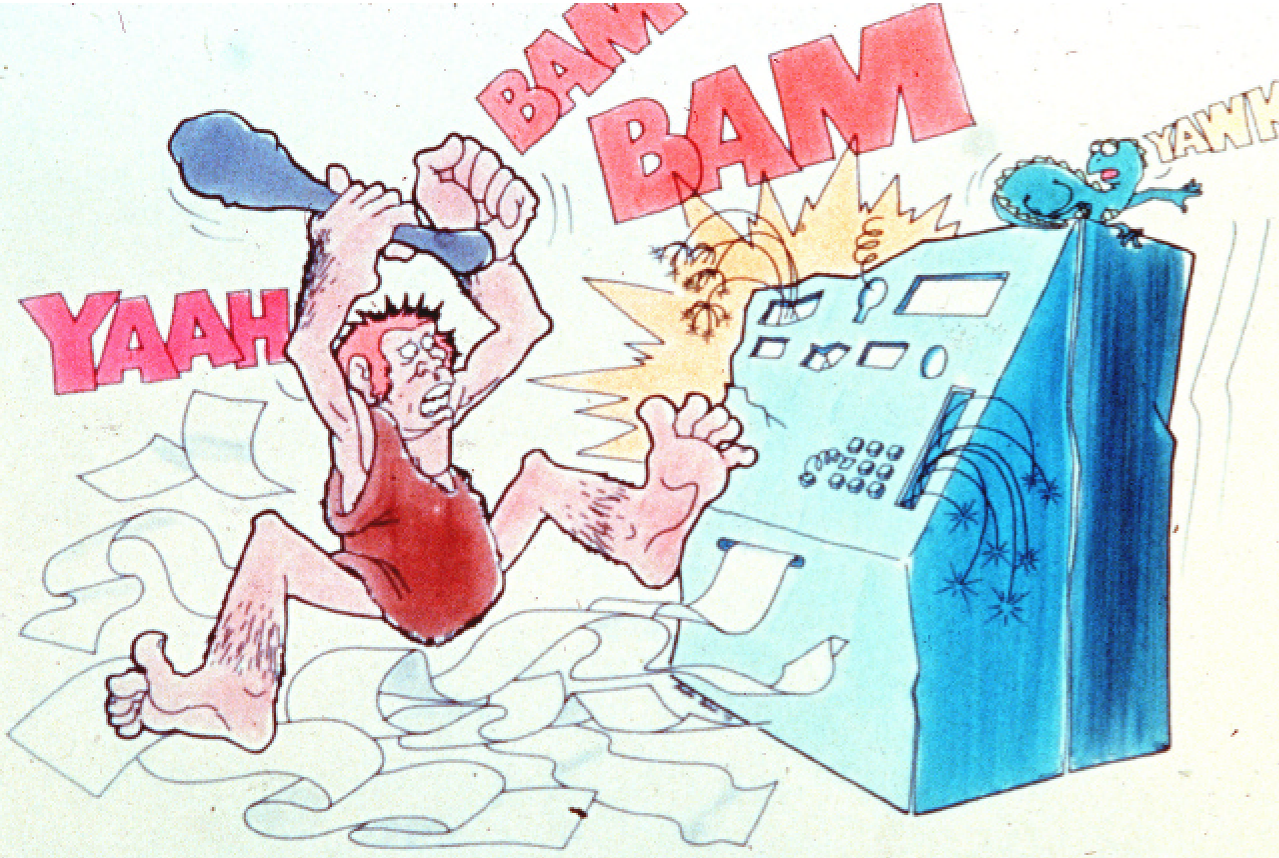


"Before computers, engineers performed computations by BRUTE FORCE"

10
5

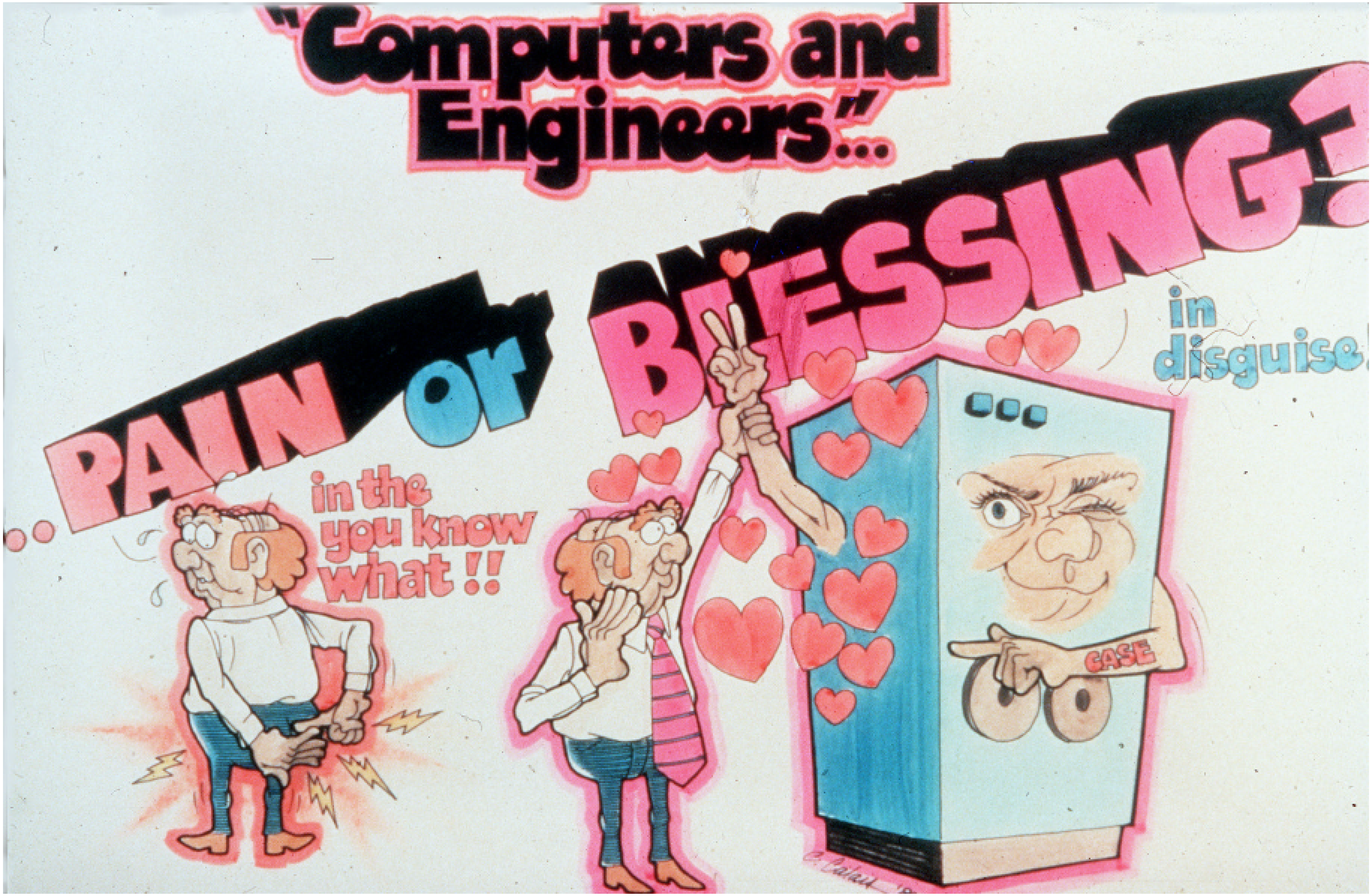

$\eta_h = \sqrt[5]{\frac{EI}{\eta_h}}$
100
$\eta_h = 1$
Axial

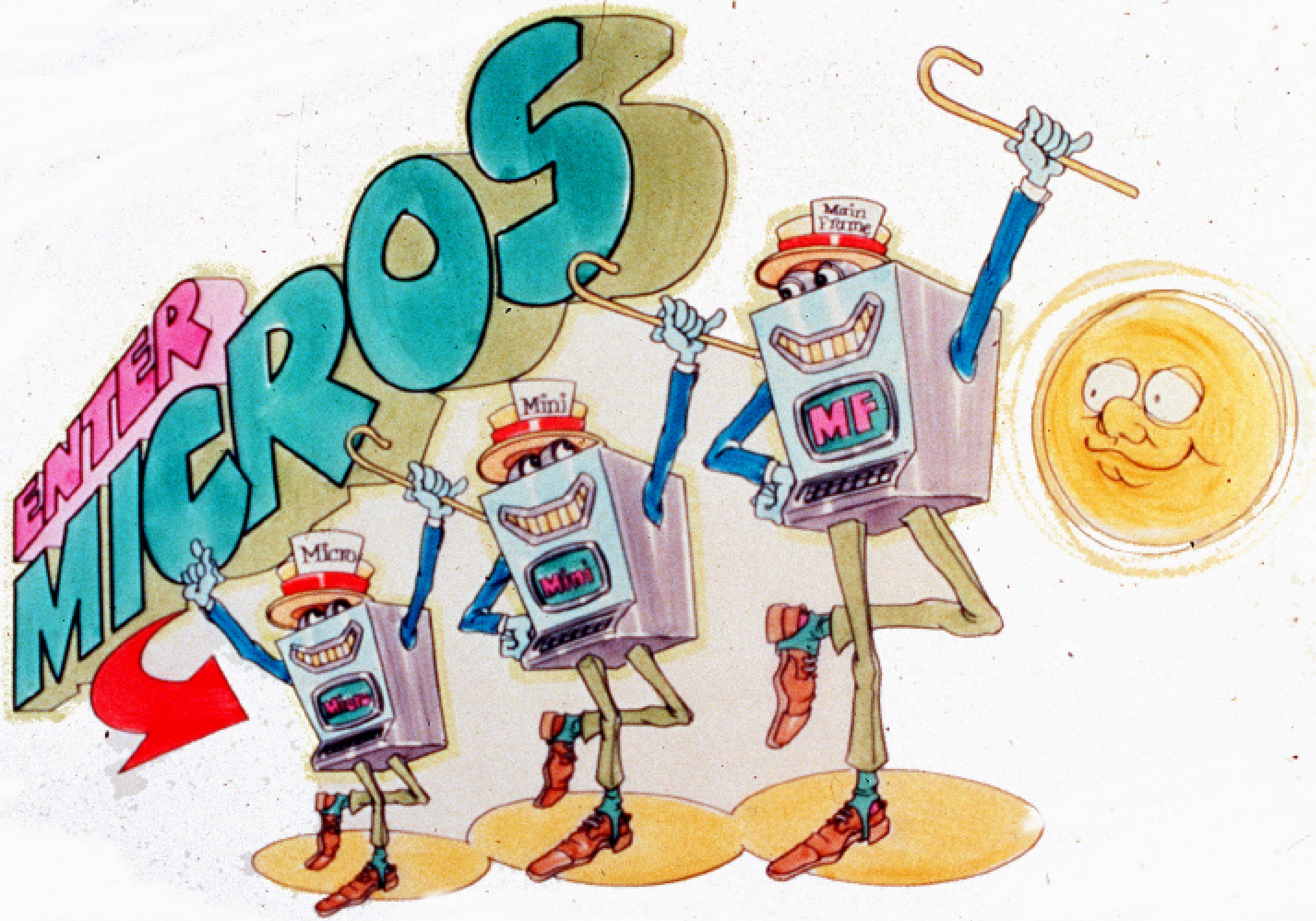
MISS JUDITH A. EILAND

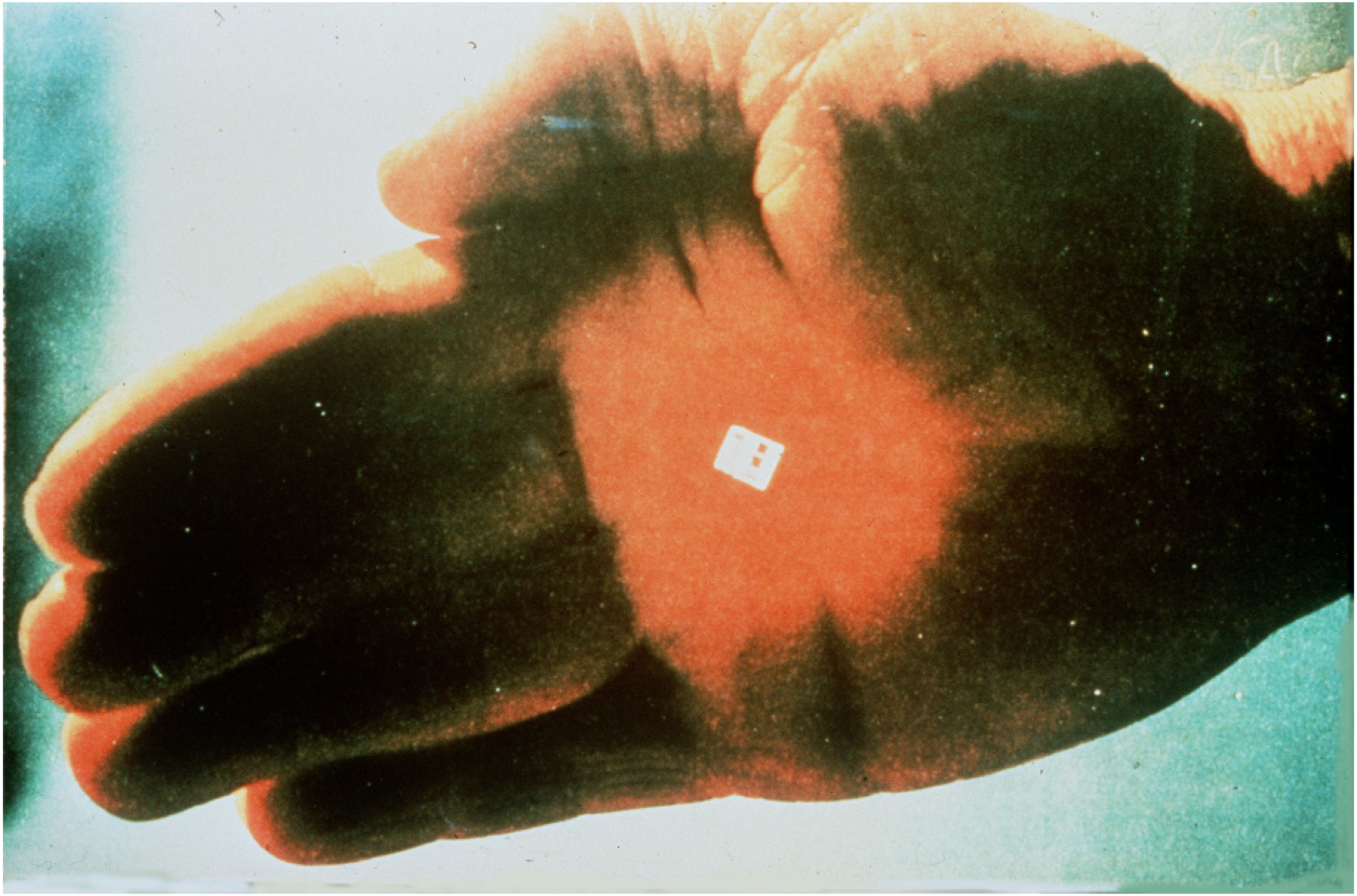


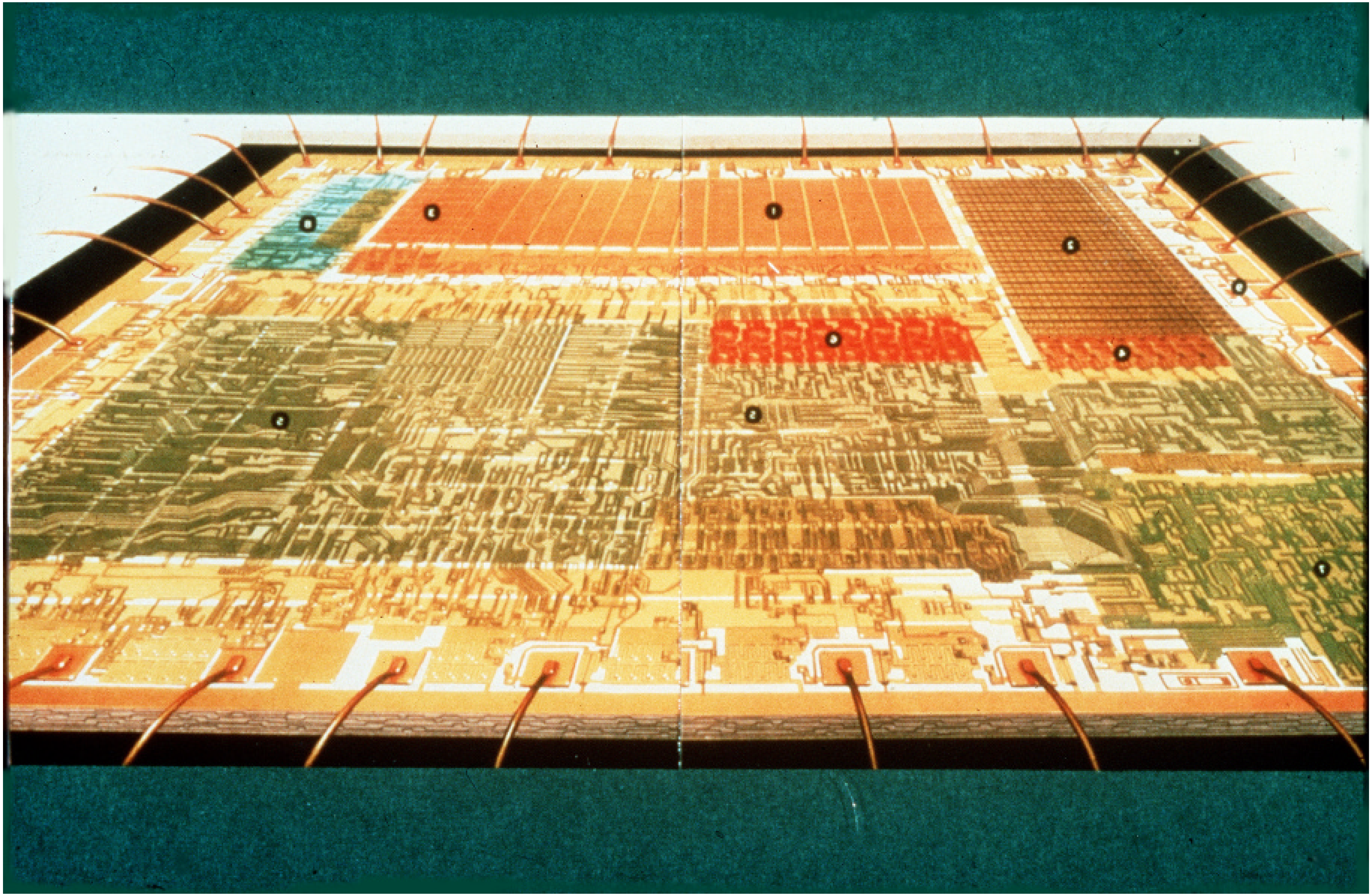
"Engineers discovered that computers were not always a **LABOR-SAVING DEVICE**"

PROMISES
PROMISES
PROMISES

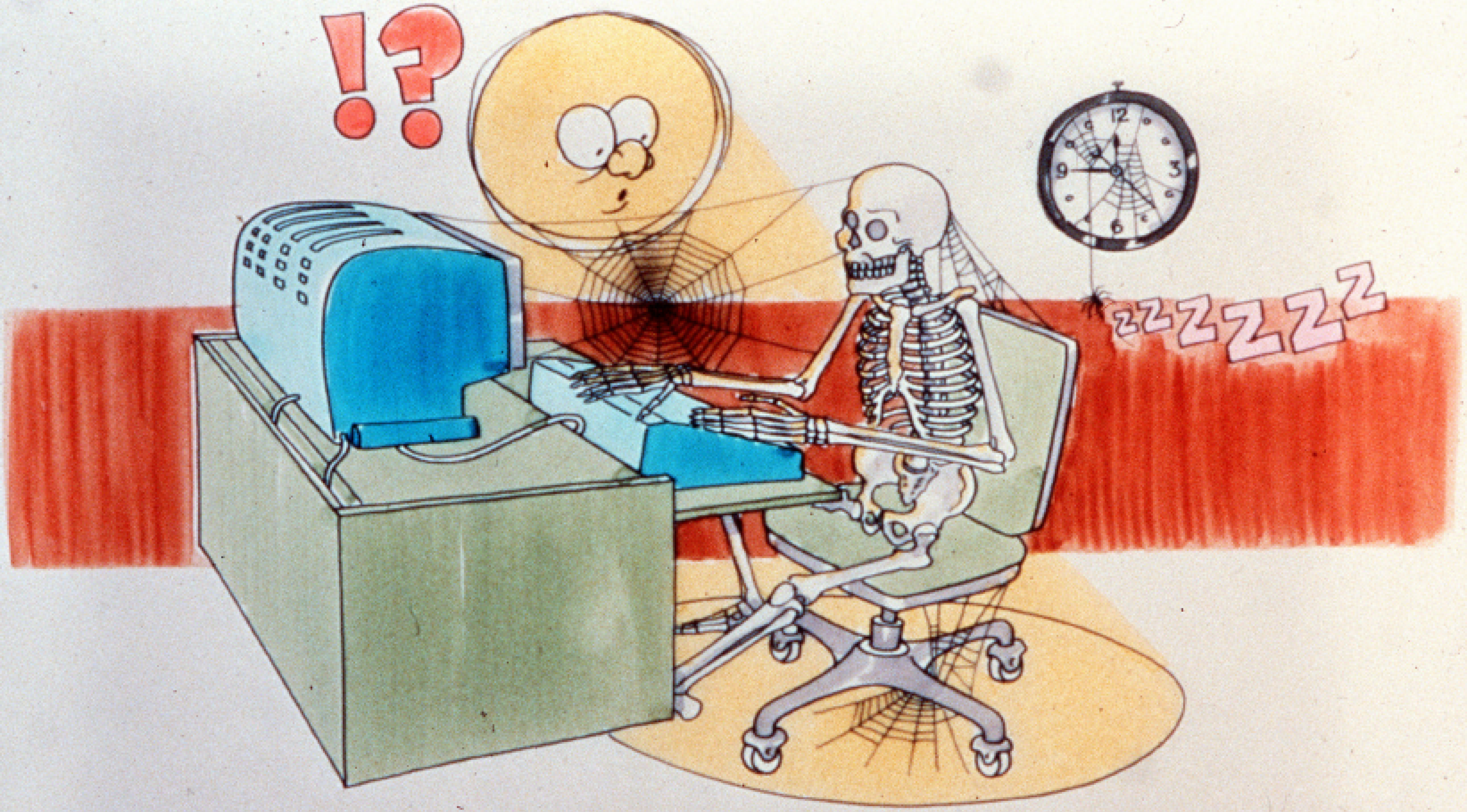

"Computers and Engineers"...
...PAIN or BLESSING?
in the you know what !!
in disguise!
CASE


ENTER
MICROS
Micro
Micro
Mini
Mini
Main Frame
MF





SHERIFF



How's the response time?!!

ROYAL
family
INTERNATIONAL mouse

Micros

A Computer Tailor made for everyone

Critical Infrastructure Protection

Protecting the critical infrastructure that provides the continuous flow of goods and services essential to the successful operation of our nation

Critical Infrastructure Services:

- Information and communications
- Electric and oil based power
- Transportation
- Water supply
- Banking and finance
- Emergency government services

Information and Communications

- In the last 5 - 10 years there has been an explosion of computing power and network technology advances altering the way information is acquired, stored, distributed and received.
- Society has an increasing dependence upon Information and Communications Technology
- Small businesses, as well as large corporations, rely heavily on current and accurate information to operate on a daily basis
- Digital information and communications has become the “backbone” of our nation’s infrastructure

Information and Communications Statistics

- Internet Domains: over 29 Million
  77% of these .COMs

- Since 1984, the number of U.S. households with one or more computers has increased fivefold

- More than 2 in 5 households have internet access (double the amount in 1997)

Information and Communications

"We have staked our way of life on the use of information. We rely more and more on computer networks for the flow of essential information. Like electricity, we now take information infrastructures for granted. Reliability breeds dependence, and dependence produces vulnerabilities."

George J. Tenet,
Director of Central Intelligence

Infrastructure Threats

- Physical threats to our critical infrastructure (attacks on property and people)
- Cyber threats to the digital information and communications component of our infrastructure

Eavesdropping on a Network

Infrastructure Threats

A serious attack on the Information and Communications Technology thread that is intricately woven into our nation's blanket infrastructure could cause an "unraveling" effect

Information Assurance

Definition

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection,and reaction capabilities.

NSTISSI 4009, August, 1997

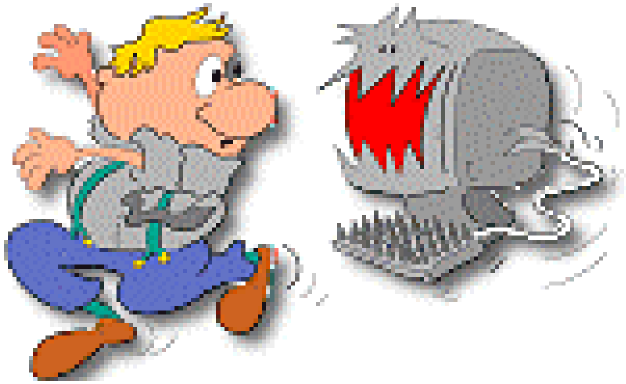
Information Assurance

- Concerned with protecting our information and communications infrastructure from external and internal threats
- Assure that information is current, accurate, authentic, and protected
- Prevention, Detection and Reaction

Information Assurance

Prevention, Detection and Reaction

You do all the right things…



…keep a careful watch...

…and react swiftly when necessary!

Information Assurance

Prevention

- Firewalls
- Passwords
- Encryption
- System Configuration Management
- Policies and Plans
- Training of System Administrators and Users
- Communication/Awareness of possible threats

Information Assurance

Detection

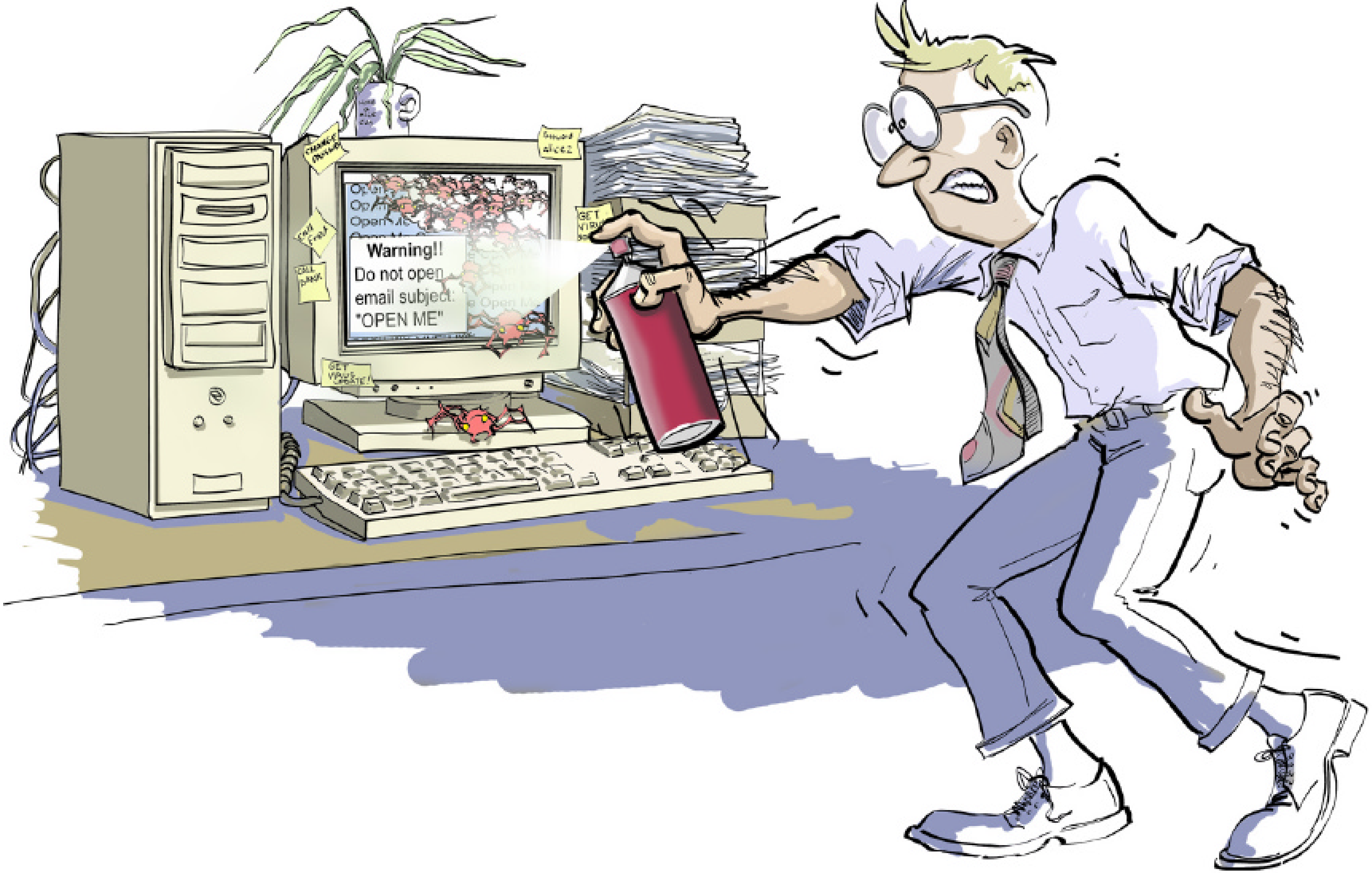
- Intrusion Detection Systems
- System Logs
- Forensic examinations of computer equipment

Information Assurance

Reaction

- “Turn out the lights” - need minimal “blocking or shutdown” points for damage control
- Analyze and patch or correct vulnerabilities on all affected systems
- Communicate necessary information to users and systems staff.

Information Assurance



The INTRUSION EXTERMINATOR

Information Assurance

- Never 100% certainty
  - Always new vulnerabilities introduced/discovered
  - Always human element (inexperience, error, oversight)
- Prudent risk management requires checks and balances
- Must react quickly to correct vulnerabilities once detected. Every second counts.

Information Assurance

- Outsider Threat - Attacks from entities outside of the country, organization, or even the household. Viewed as malicious hackers from “out there”.
- Possible:
  - Terrorists
  - Intelligence agencies
  - Criminal groups
  - Competitors
  - Hackers

Information Assurance

Outsider Threat

- Several foreign countries are known to be training their intelligence officers to hack into U.S. computers
- Due to the interconnectivity of the world’s information and communications infrastructure, an expert hacker can weave through dozens of computers across many countries undetected.
- Through the use of low cost, low risk intrusion tactics, small countries now have the ability to engage in information warfare against other highly developed nations.

Information Assurance

- Insider Threat - Attacks from inside the organization. Someone with authorized access to computer systems and networks.
- Possible:
  - Disgruntled employees or contractors
  - Employees who are deliberate plants or “spies”
  - Employees who are knowingly or unknowingly manipulated or pressured

Surveys show that greatest threat comes from the insider. Estimated that 80% of all attacks are from within an organization

Information Assurance

Insider Threat

- Often **more harmful** than attacks from outside and **more difficult to prevent** because intruder has inside information and system privileges available only to authorized users
- Use social engineering tactics to manipulate employees and gain access to systems by preying upon an insider’s human nature to be helpful or their lack of security knowledge.

Information Assurance

Three Levels of Security

Need to authenticate

- Who you are
- What you know
- What you have

This can be accomplished through multiple systems or identifiers

Information Assurance

Additional Measures of Prevention For Insider Threat

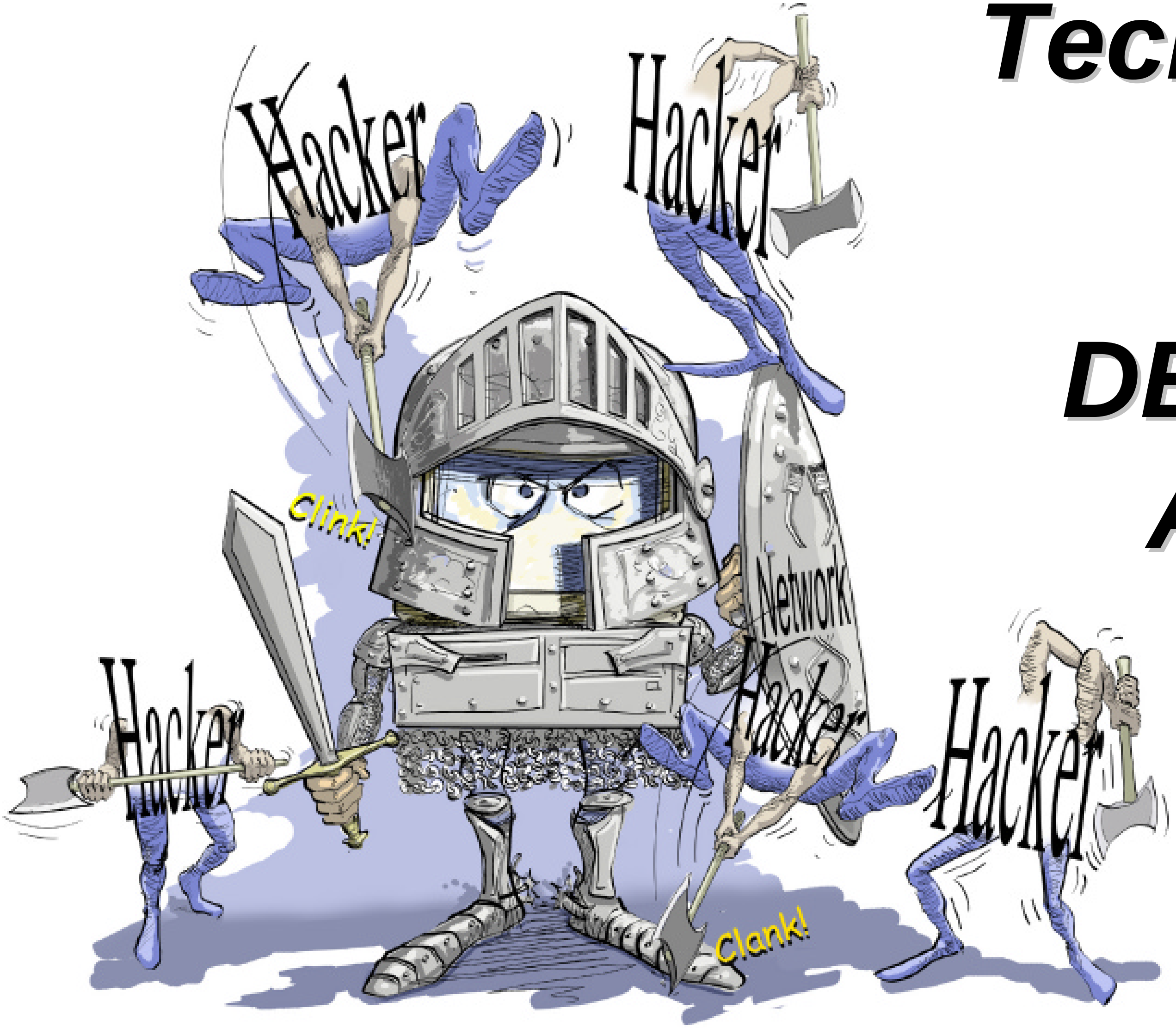
- Educate users about security practices and the dangers and tactics of information warfare
- Profile system users
- Background checks of systems administrators
- 100% activity log to capture all system/network activity for forensic investigations
- Additional computer security technology (PKI, biometrics, smart cards, digital signatures, time/date stamping)

Information Assurance

Computer Security Technology

- Public Key Infrastructure (PKI) – a comprehensive encryption system with security management, authentication controls, system integration, and data recovery capabilities
- Biometrics – systems to authenticate user (retinal scans, fingerprints, face recognition)
- Smart Cards – hardware implementation of PKI for greater security. (Embed PKI chip onto card)
- Digital Signatures – authentication of identity, provides assurance of message integrity
- Time/Date Stamping – trusted third-party stamping to provide an authentic chronological trail

Computer Security Technology



DEFENSE Against the Enemy

Information Assurance

Army Research Laboratory (ARL) IA Program

- Center for Intrusion Monitoring and Protection (CIMP)
  - conducts Information Assurance function for DoD/Army/ARL
  - operates to safeguard corporate business and scientific research information
  - research component for developing new tools for detection, protection and analysis. Enhancements to improve the process
- Tactical Information Assurance Research

Information assurance is vital both for the battlefield and the corporate infrastructure

Information Assurance

ARL Center for Intrusion Monitoring and Protection

- Protecting customers with comprehensive intrusion detection tools
- Operationing element coupled with a process improvement component
- Capturing traffic data at inter-network connection points and selected sites
- Technology transfer to other DoD/Army agencies
- Partnership with Army Reserves provides additional capability of weekend monitoring and analysis.

Information Assurance

ARL CIMP Environment

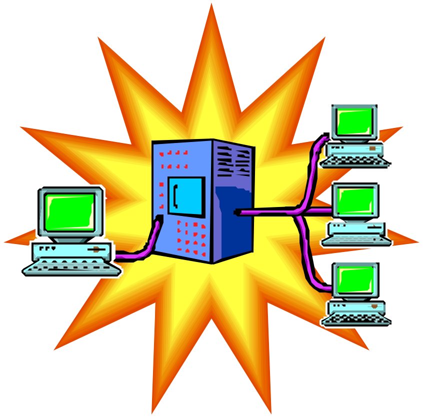
- Distributed and Diverse IA Customers
  - Defense Research & Engineering Network (sends and receives between 2 and 3 Terabytes per day, w/all IA performed by ARL)
  - DoD High Performance Computing Modernization Program Army Materiel Command, Army Research Laboratory (45 sites, thousands of users)
- Heterogeneous Computing
  - High performance computers (a world's top 5% HPC center), parallel, vector, and cluster systems
  - Thousands of workstations & PCs
  - UNIX (> 10 variants), LINUX, NT/2000, Windows
- Heterogeneous Networking
  - LANs: ATM, FDDI, HIPPI, Ethernet, Wireless
  - Protocols: TCP/IP, IPX, RPC, Multicast, Mobile Ad Hoc
  - External Connections: DREN, NIPRnet, SIPRnet, Internet

Information Assurance

ARL CIMP Program Strengths

Tight coordination and involvement between the CIO and Intelligence and Security operations

Since the toolset is immature, close coupling with a strong R&D environment hastens technology development, and facilitates transfer to fielded intrusion detection systems



Strategic partnerships:
US Army Reserves
Universities
Other Government agencies
Industries

Information Assurance

ARL Tactical Research Program

- Technologies to effect secure communications and networking for wireless tactical environments
- More difficult than operational IA environment, involves wireless communications with auto addressing and self configuring networks
- Important technology for Future Combat System (FCS)

Supported by:

- Collaborative Technology Alliance (CTA)
- Multidisciplinary University Research Initiatives (MURI)
- ARL Broad Agency Announcements (BAA)
- In-House Research Projects

Information Assurance

ARL Tactical Research Program

Focus areas:

- Computationally-efficient intrusion detection techniques
- Automated intrusion detection and vulnerability assessment tools
- Highly efficient security services
- Highly efficient security infrastructure (e.g. distributed shared-key generation/management techniques, adaptive data authentication)
- Security management for noisy, low-bandwidth tactical networks

Information Assurance

ARL Tactical Research Program

Challenges:

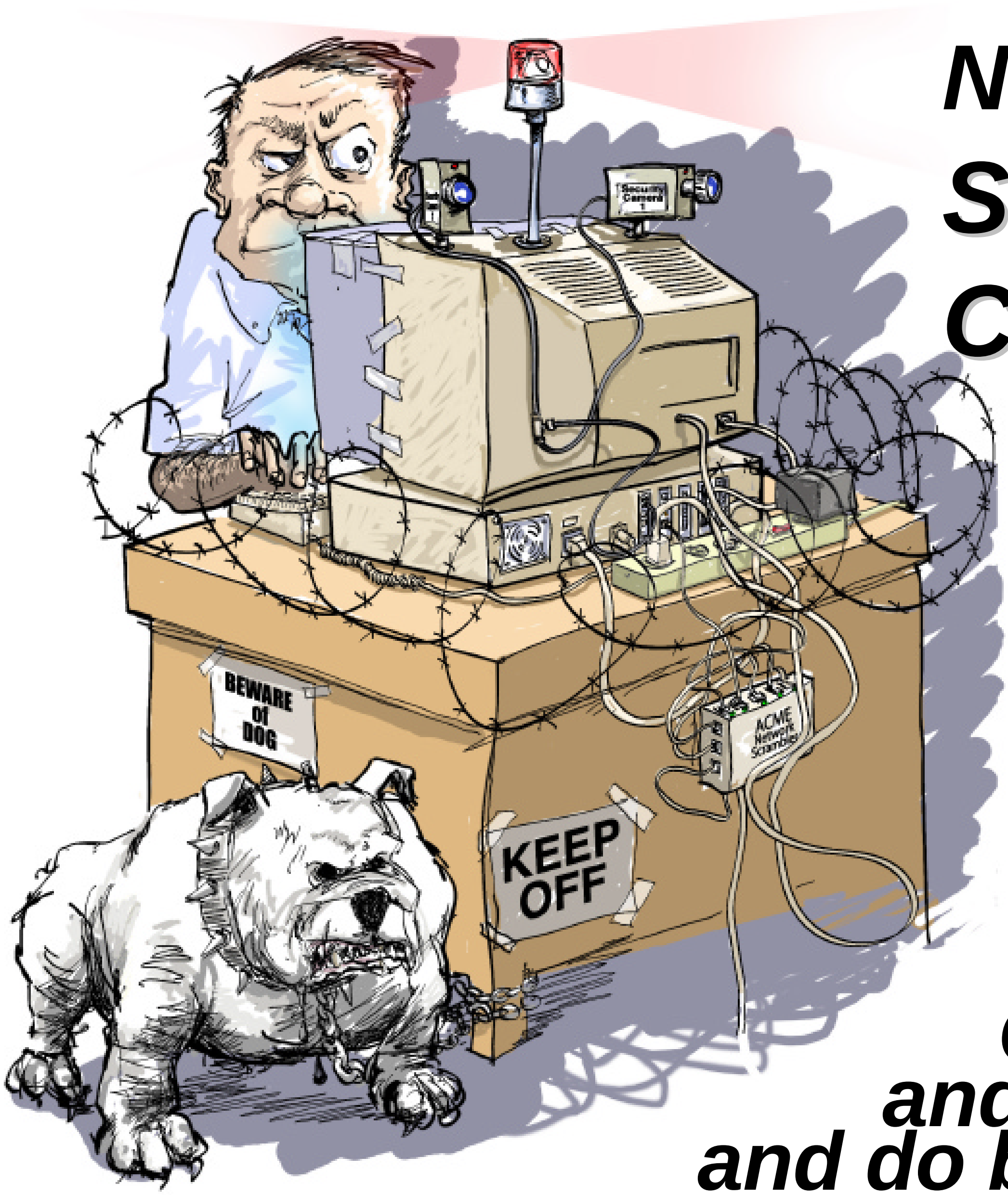
- Technologies that are real-time, automated, scaleable, efficient, adaptive, and secure
- A mobile, dynamic network infrastructure
- Capability for self-configuration and auto-addressing
- Mitigating noisy channels, interference, and jamming
- Adapting to changing channel conditions and network topologies
- Overcoming severe constraints in bandwidth, power and energy

Information Assurance

Test and Evaluation

- The same level of security and detection practices apply to the T&E community
- In addition there is a need for strict coordination and communication of testing guidelines and measurements for evaluating IA related hardware and software
- As new vulnerabilities are discovered, swift action must be taken to communicate new test evaluation criteria to the field and determine if re-testing is a requirement

Need to be more
SECURITY CONSCIOUS



Changing culture and the way we live and do business

Information Assurance

Challenge

- Many known vulnerabilities exist across varying computer platforms
- Intrusion detection functions being performed and vulnerabilities reported from multiple levels of government and industry players with no central repository
- Vast amounts of data concerning possible and real threats exist in this country with no mechanism for organizing the information and gaining insight into future developments

Information Assurance

Before September 11

- Minimal funding for computer security, in both government and industrial environments
- Focused on making computer systems more secure as opposed to using monitoring and detection techniques
- Extraordinary effort on Y2K, with minimal impact, left our country feeling less than enthusiastic about continuing computer security hype

WATER WATER EVERYWHERE
AND NOT A DROP TO DRINK!
splash!
WATER

Information Assurance

Since September 11

“We face new threats and therefore we need new defenses for our country. We face a united and determined enemy, we must have a united, determined response. In the war on terror, knowledge is power.”

- President George W. Bush

Information Assurance

Since September 11

- Increased emphasis on protecting our infrastructure
- Chance of further attacks, both physical and cyber, is certain
- Increase in threats to the internet
- Experts are calling for increased government coordination and centralization of information security efforts
- Bill passed through the House on Feb. 7 calling for the federal government to spend $880 million over the next five years in support of computer security research

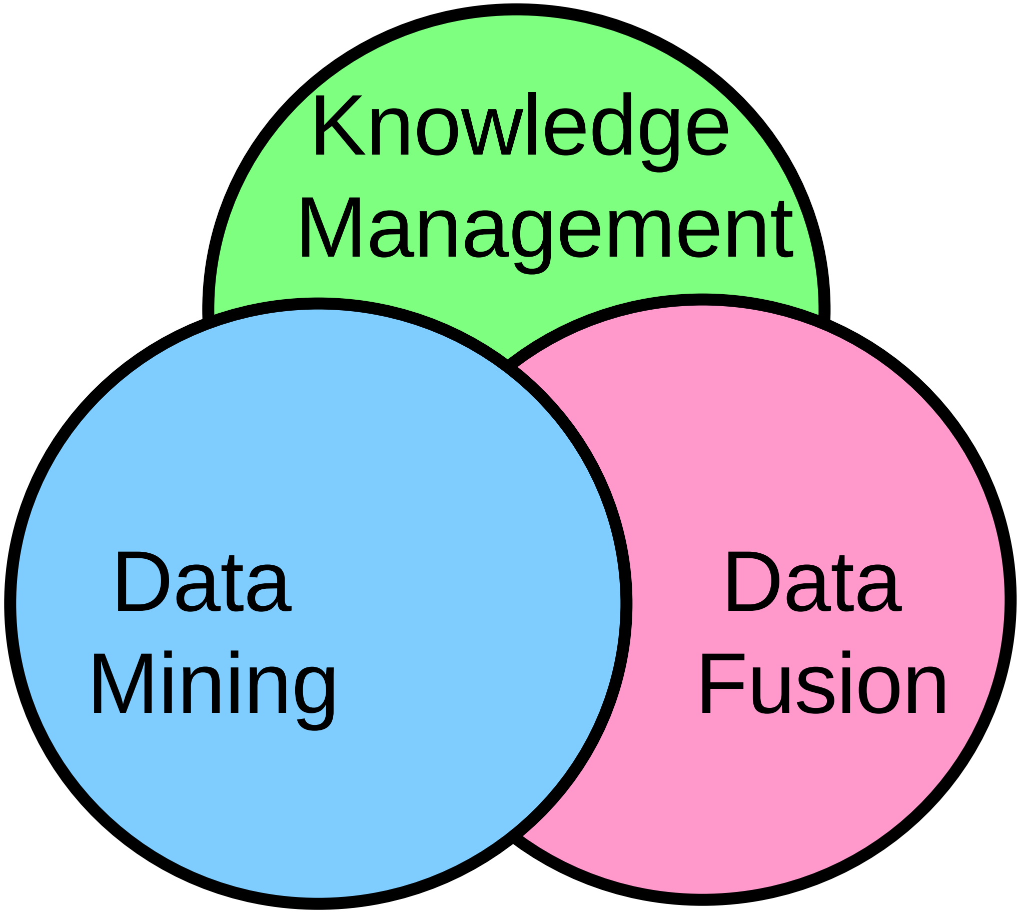
Information Assurance

“An immense and ever-increasing wealth of knowledge is scattered about the world today; knowledge that would probably suffice to solve all the mighty difficulties of our age, but it is dispersed and unorganized. We need a sort of mental clearing house for the mind: a depot where knowledge and ideas are received, sorted, summarized, digested, clarified and compared.”

- H.G Wells in “The Brain: Organization of the Modern World”, 1940

Information Assurance

Knowledge Discovery



Information Assurance

Knowledge Discovery

- **Data Fusion**- the seamless integration of distributed and disparate sources of data

- **Data Mining**- computational techniques and methods for extracting useful information from billions of bits of data.

- **Knowledge Management** - methods for managing and gaining knowledge from useful information (visualization, pattern recognition, classification, AI technology)

Infrastructure Assurance Technology and Analysis Center

There is an urgent need for:

- Better technologies to detect & prevent intrusions
- Better technologies to identify perpetrators
- Better technologies for knowledge discovery, visualization, and decision support
- A Center for conducting incident analyses and disseminating findings
- A common Incident Database
- A standard Information Assurance process

Infrastructure Assurance Technology and Analysis Center

There is an urgent need for (cont):

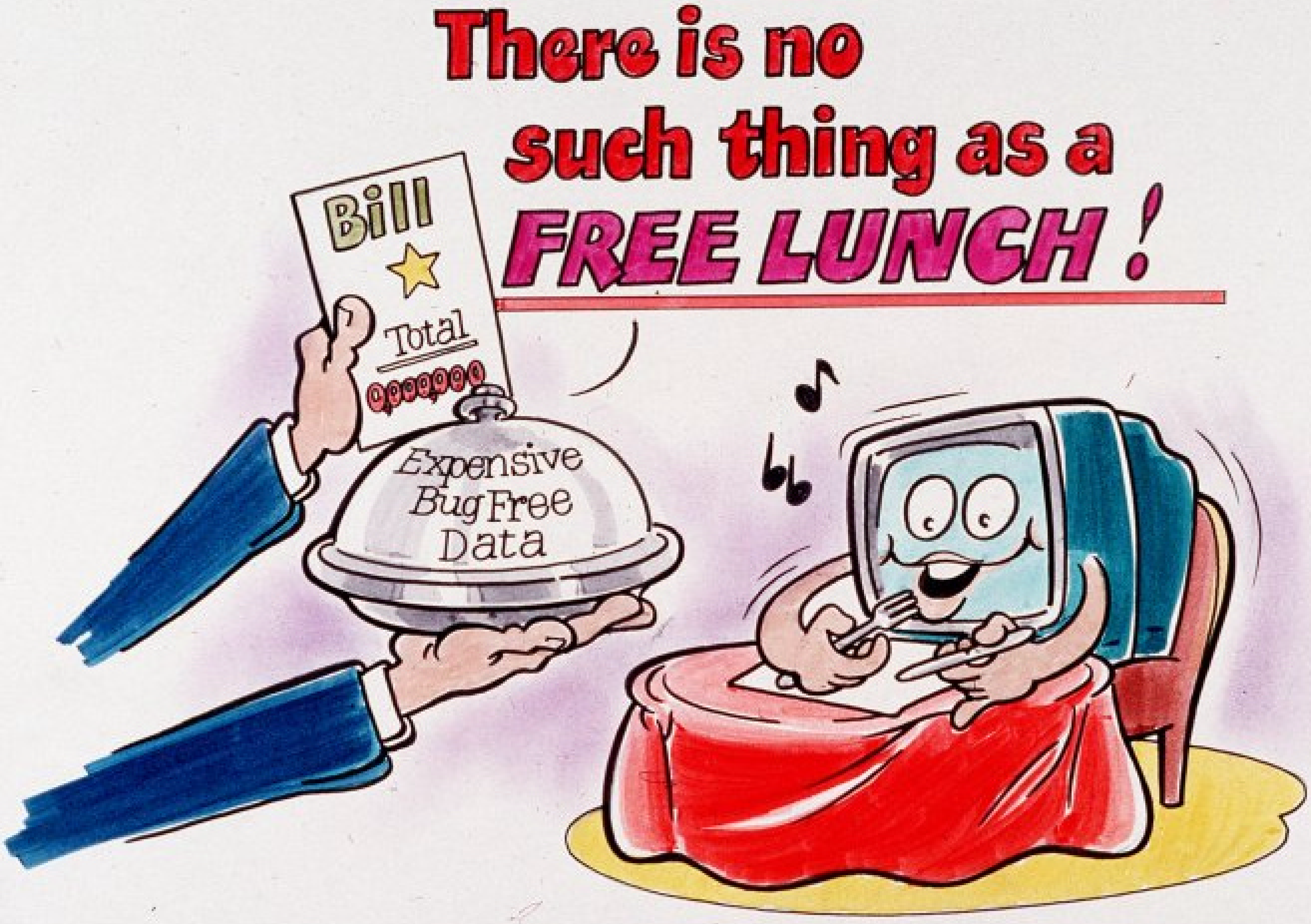
- a coordinated, effective IA program that synergistically utilizes IA contributions from the Services, DISA, NSA, DARPA, other government agencies, industry and academe
- coordinated IA research that promotes and facilitates collaboration among the best & brightest in government, academe and industry

Infrastructure Assurance Technology and Analysis Center

Government — Provides management oversight, requirements, in-house research expertise, test beds, and real world training for faculty and students

Academia — Provides basic research, academic training

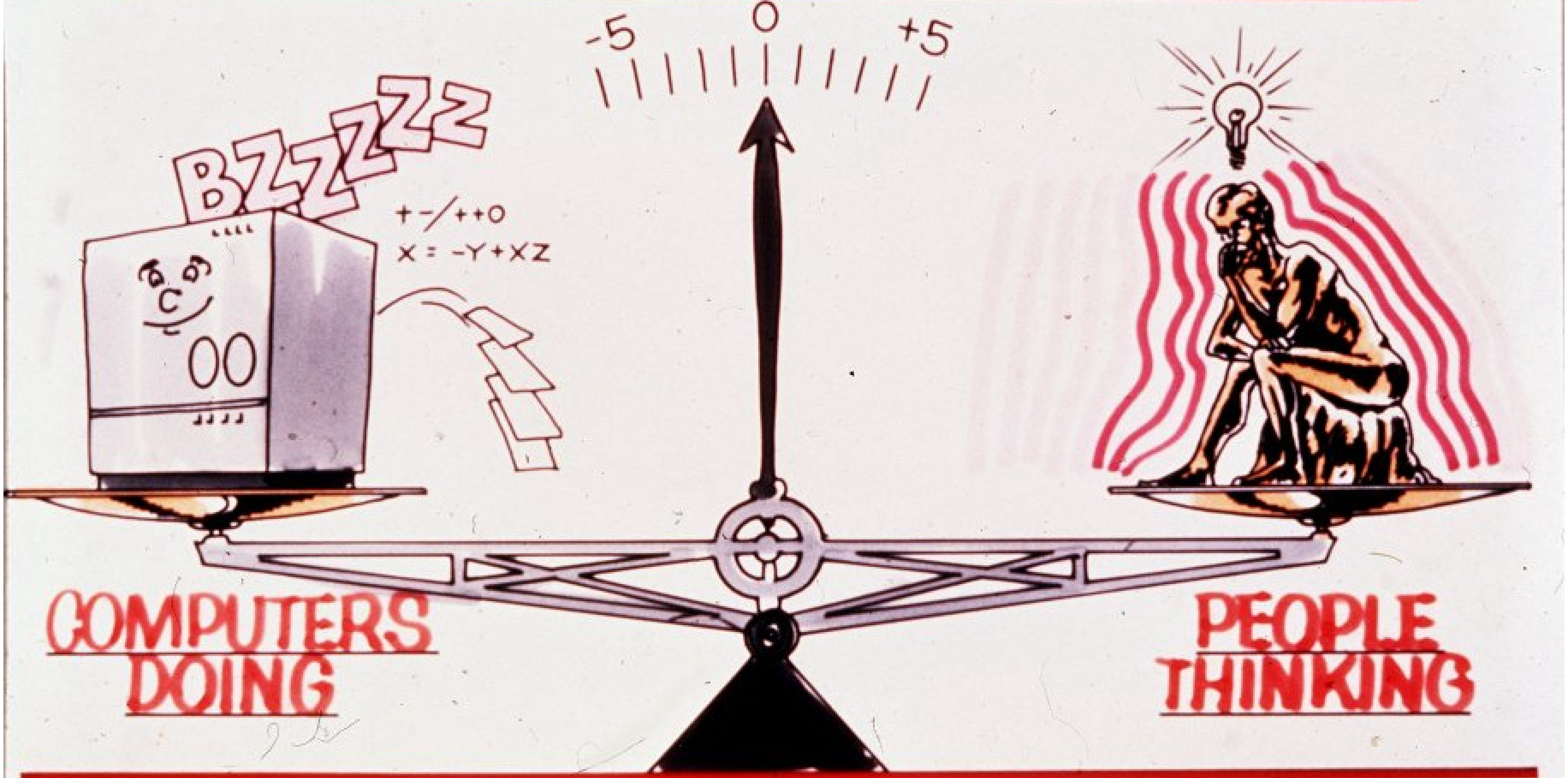
Industry — Provides technology transfer, commercial applications, industry requirements

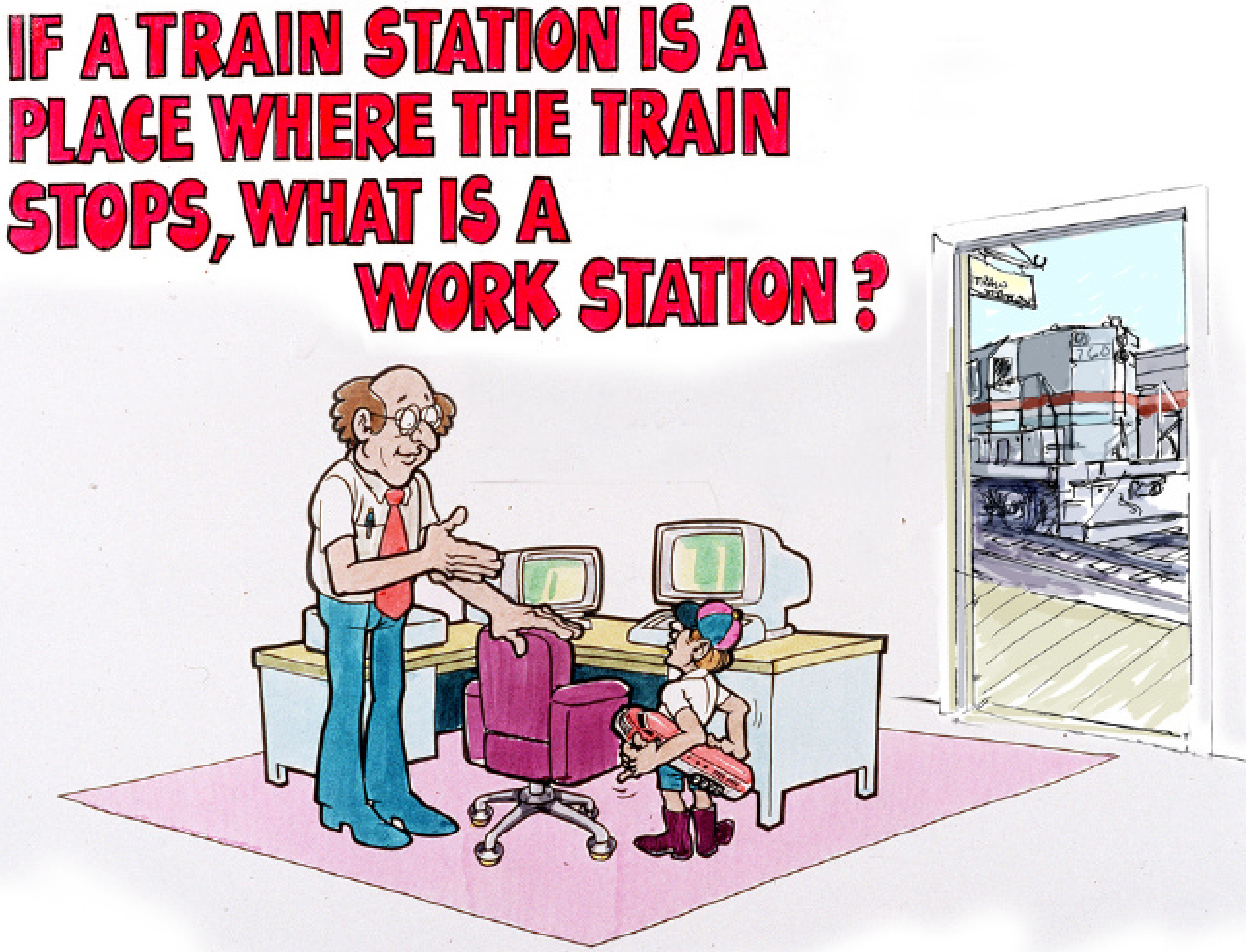

There is no such thing as a FREE LUNCH!
Bill
Total
Expensive Bug Free Data

Information Assurance

Always remember, as technology advances and our capabilities increase, so do the tools of our adversaries. The techniques we use for intrusion detection and knowledge discovery can also be used by our enemy to provide insight into our lives and our vulnerabilities. This threat is a continuing one and we must treat it as such.

A WELL BALANCED EFFORT




IF A TRAIN STATION IS A PLACE WHERE THE TRAIN STOPS, WHAT IS A WORK STATION ?